The GLOCEPS

Weekly Influential Brief

Shifting patterns of illicit financial flows in Kenya

Executive Summary

This brief examines the shifting dynamics of illicit financial flows in Kenya. It focuses on trade-based and faith-based money laundering (TBML & FBML) practices, obstacles to the Ultimate Beneficiary Registry (UBR), the impact of online merchant settlements (OMS), the advent of Central Bank's Digital Currency (CBDC), crypto-currencies, and exposure of fintech firms to money laundering (ML). The brief advances the escalation of deceptive trade especially in the tea industry and ivory trafficking, and explores the growing exposure of religious entities to ML, in addition to the rise in OMS as a conduit for ML due to potential laxity in customer due diligence. It examines, the introduction of the CBDC and the proliferation of crypto-currencies furnish novel ML avenues as criminals leverage their decentralized nature and potential for anonymous transactions. The escalating presence of the less regulated fintech entities, compounds the complexity of mitigating illicit financial flows. This places Kenya as a strategic hub in the growing space that is global ML.

Recommendations

The brief recommends that county governments should;

a) the establishment of a comprehensive regulatory framework tailored to the digital payment sector.

b) extension of industry practices to religious organizations, including Know-Your-Customer (KYC) due diligence.

c) extensive awareness campaigns to educate entities and individuals on their obligations,

d) promotion of Ultimate Beneficiary Ownership (UBO) reporting.

Shifting patterns of illicit financial flows in Kenya

Full Brief

Introduction

The Kenyan economy is undergoing a notable transformation, marked by shifting patterns in illicit financial flows. Factors driving these realities include weak regulatory frameworks, corruption, and the exploitation of financial sectoral vulnerabilities. Of particular concern is the leveraging of technological advancements like digital payment systems and virtual currencies for ML. Collectively, they pose challenges to the integrity and stability of Kenya's financial system.

In light of these developments, the paper delves into the evolving landscape of ML. Understanding these dynamics is central to mitigating associated risks like distortion of market prices and financial systems. Through the in-depth analysis of these elements, this paper provides a comprehensive insight into the emerging complexities of ML in Kenya. Furthermore, it offers actionable recommendations for policy-makers, regulators, and stakeholders alike in bolstering AML efforts. Through collaborative efforts and evidence-informed strategies, Kenya can combat illicit financial flows and safeguard her financial system.

Context

Money laundering in Kenya persists as a significant challenge. According to Kenya's National Risk Assessment (KNRA), Kenya faces a medium level of ML risk and a potential for escalation. The updated AML legislation in 2023 is one of the strategies employed to address limitations in previous anti-money laundering undertakings. This gap was highlighted by the Financial Action Task Force (FATF). This has resulted in Kenya being placed on the global financial watchdog's "gray list" in 2024.

Of particular concern is the finance system vulnerabilities in Kenya's banking sector. Sectors such as real estate, money network operators (MNOs), saccos, and legal and motor vehicle dealers are potential exposure points derailing AML efforts.

The investigation and prosecution of money laundering offenses remain weak. The implementation of a risk-based approach, oversight of non-financial businesses and professionals, and efforts to administer penalties face challenges. Consequently, Kenya has become a hub of corrupt entities seeking to conceal illicit cash flows. The government's sponsoring the relaxation of AML reporting thresholds will exacerbate vulnerabilities.

Addressing money laundering and related financial crimes remains imperative for fostering a stable economy and sustainable growth. However, the increasing price of real estate and high-value luxury items may signify layering tactics at play. To this end, Kenya must undertake comprehensive risk assessments on activities tied to high-value proceeds of crime. While Kenyan authorities have achieved some success in recovering proceeds of crimes stored locally, international recoveries remain insufficient.

Kenya has made significant strides in meeting International Anti-Money Laundering (AML) standards since the enactment of the Amended Proceeds of Crime and Anti-Money Laundering Act of 2023 (POCAMLA). Detecting emerging ML threats and trends remains imperative, particularly those intertwined with new technologies, TBML, FBML, and enhancing the efficacy of of the Ultimate Beneficiary Registry.

Research Methodology

To understand the evolving patterns of illicit financial flows in Kenya, qualitative data was gathered through interviews with expert respondents using structured interview guides. This primary data was supplemented by documented secondary data. Thematic analysis was undertaken to examine and interpret the collected data, allowing for a comprehensive exploration of the shifting dynamics in illicit financial activities in Kenya.

Key Issues

The discussion on evolving patterns in ML activities revolved around several key issues. These include TBML, FBML, the implementing challenges on the UBR, and advancements in the digital finance sector.

Trade-based money laundering (TBML)

Criminals employ TBML to obscure the origins of illicit funds. It is concurrently being used to layer proceeds from drug and human trafficking, and weapons smuggling. This tactic involves disguising the proceeds of illegal activities as legitimate trade transactions. Criminal entities employ skilled personnel like lawyers and accountants to launder money through trade, including manipulating involves, falsifying trade descriptions, and utilizing shell companies.

In 2018, significant instances of import under-invoicing were observed in key product categories such as minerals, fuel, electric machinery, vehicles, cereals, and used clothing. Similarly, on the export front, mis-invoicing was recorded in the trading of export commodities like coffee, tea, and spices. The tea sector has been targeted by criminal syndicates to smuggle ivory.

The proliferation of small and medium-sized enterprises has facilitated the rise of ML. Restaurants, private hospitals, pharmacies, and wholesale shops are attractive platforms are they deal in cash. Their location in high-traffic areas makes it easier for them to justify large cash transactions, possibly from illicit financial transactions.

A surge in mobile money amplifies the avenues for TBML. Mobile money options and global payment applications are used to over-or under-invoicing goods and services. Criminal elements capitalize on them to evade detection due to the absence of mechanisms to authenticate the legitimacy of such transactions. They exploit the mobile money ecosystem to convert and seamlessly transfer electronic cash and other assets across borders.

Faith-Based Money Laundering (FBML)

FBML is a nascent facet of illicit financial flows. Patterns and dynamics are shifting to the utilization of religious institutions as conduits for ML.

Religious leaders are revered as moral and sacred. However, they are not immune to financial malpractice. They are either willing or coerced collaborators to FBML operations. The phenomena of FBML encompasses a myriad of activities where funds from corrupt sources are seamlessly integrated with legitimate finances, under the guise of religious contributions and donations.

Sources are generally undisclosed.

The unregulated environment within which religious organizations operate is a key driver to FBML. This facilitates an influx of funds without the requisite scrutiny or oversight.

Criminals also embed themselves in religious organizations to perpetuate financial fraud by exploiting the lack of stringent accounting mechanisms. Others hold positions within both the criminal and religious worlds, hence using their position to commingle illicit proceeds with legitimate contributions. Moreover, they exploit the trust of congregants to undertake FBML, further complicating detection and mitigation. While FBML is perpetuated by all religious denominations, the Christian faith is susceptible. They bear the brunt of monetary dishonesty.

FBML has been reported in other jurisdictions like the United States. There, religious groups are exempted from stringent reporting requirements, including federal tax filings. The resulting lack of transparency underscores the urgent need for enhanced regulatory measures and accounting mechanisms to combat the challenge of FBML.

Similarly in Kenya, FBML has been documented. Bank accounts of religious entities have been frozen as they are suspected of ML. Investigations have unveiled the multifaceted nature of FBML and transnational organized crime. These range from radicalization, murder, child abuse, and potential organ trafficking.

Effectively addressing the phenomenon of FBLM necessitates navigating the delegate balance between religious freedoms and safeguarding financial integrity. It calls for concerted efforts to bolster AML measures including robust Know-Your-Customer (KYC) protocols and enhanced regulatory oversight to stem the tide of illicit financial flows within religious institutions.

Ultimate beneficiary registry

Criminals use shell companies to obscure ownership of traded goods and conceal the origin and destination of funds. The Ultimate Beneficiary Registry (UBR), established under the Companies (Beneficial Ownership Information) Regulation of 2020, mandates companies to disclose their ultimate beneficial owners (UBOs) to the Registrar of Companies. The UBR provides a centralized repository of ownership information thus aiding in the prevention and detection of ML and other illicit activities.

Despite its potential, UBR implementation is challenged. It faces low awareness among companies and difficulties in obtaining accurate UBO information. This leads to low compliance levels. Criminal groups may exploit the registration process by providing false information about employing nominee entities to blur the ownership or control of companies, further impeding the government's efforts to trace the origins of illicit funds. Lack of coordination among government agencies poses risks of duplication and inconsistencies in data collection which can potentially be exploited by criminals.

Moreover, apprehensions over the security and privacy of UBR data have heightened the risk of exposure to cybercrime. The UBR database houses critical information about business owners, hence concerns over unauthorized access and malicious exploitation. Breaches could facilitate identity theft, enabling criminals to establish fictitious companies or manipulate existing ones to facilitate unlawful transactions.

Manipulation of UBO information in the UBR database enables money launderers to create false trails which complicate the tracing of the true beneficiaries of illicit funds. Phishing tactics, where criminals undertake social engineering attacks to steal user data such as login credentials, pose the risk of extracting sensitive information from the UBR, potentially compromising the database's integrity or facilitating fraudulent activities. Urgent measures to address these challenges are imperative for securing the UBR's efficacy in combating ML and related crimes.

Advancements in the digital finance space

Progression in Kenya's digital financial space has significant implications for ML activities. Several pertinent issues emerge in this context:

a) Increased online merchant settlements

The proliferation of virtual assets and transactions, compounded by the absence of a corresponding regulatory framework poses a substantial challenge. Technological evolution has spurred the growth of digital marketplaces. However, the anonymity inherent in virtual transactions facilitates opportunities for money launderers to conceal their activities. The absence of physical presence complicates identity verification, thus increasing the susceptibility to fraudulent activities.

The borderless nature of online transactions exacerbates regulatory challenges. It makes it arduous for authorities to monitor cross-border funds flow promptly. Consequently, the swift nature of virtual transactions hampers the regulator's ability to identify suspicious patterns and activities promptly.

b) Central Bank Digital Currency (CBDC)

Kenya's consideration of adopting a digital currency introduced new dynamics to ML. The Central Bank Digital Currencies (CBCD) offers heightened anonymity. Moreover, instant cross-border transactions facilitated by the CBDC have the potential of being employed to circumvent traditional banking systems and regulators who can be overwhelmed due to capacity challenges. Money launderers could exploit the CBDC to layer illegal funds through intricate and obscure transactions.

Integration of the CBDC with the financial systems portends to commingling of illicit and legitimate funds, elevating the ML. Additionally, the CBDC operating on digital platforms is vulnerable to cyber-attacks. Data breaches and system manipulation may be exploited for ML.

c) Cryptocurrency

Crypto-currency adoption in Kenya presents a conundrum, with weak regulations encouraging criminal exploitation. Despite the Central Bank's caution against dealing with cryptocurrencies, the Capital Market Authority has proposed regulations, signaling a growing acknowledgment of its potential and risks. The absence of a comprehensive legal framework leaves regulatory gaps that could enable criminals to exploit unregulated platforms.

Cryptocurrencies' decentralized nature and anonymous transactions present challenges in tracking illicit activities, enabling criminals to launder money discreetly. Moreover, the use of digital wallets further complicated the tracing of funds, exacerbating the challenges of combating crypto-currencies-related money laundering in Kenya.

d) Rising number of fintech

The proliferation of unregulated fintech companies presents a concerning trend. Emerging fintech start-ups lack robust customer due diligence procedures, providing an avenue for ML on their platforms.

Their global integration enables seamless transfer of funds, making it harder for regulators to monitor transactions. The comparatively lighter regulatory oversights on fintechs to those of traditional financial institutions render them attractive targets for ML. A notable instance is the ML investigation of Flutterwave in Kenya. The adoption of advanced financial technologies in fintechs makes them appealing to criminals interested in blurring monetary transaction histories. This potentially creates hurdles for law enforcement agencies in combating ML.

Kenya has emerged as a conducive environment for new fintechs due to the robust local mobile payment infrastructure, widespread smartphone adoption, and large unbanked populations. The benefit from a vibrant entrepreneurial ecosystem, access to funding opportunities, and a tech-savvy population contribute to her appeal as fintech start-ups seek to innovate and expand their businesses.

The government has demonstrated support for the fintechs through initiatives like the regulatory sandbox. This offers a controlled environment for experimenting with new portfolios. While the sandbox fosters innovation, it also introduces ML risks. Regulatory bodies may grant certain oversight exemptions for participating fintechs. This could create an environment where illicit financial activities.

Conclusion

The evolving patterns of illicit financial flows in Kenya underscore the multifaceted nature of ML and the challenges in combatting them effectively. TBML and FBML have emerged as prominent avenues for concealing illicit funds as they exploit vulnerabilities and limitations in regulations. While initiatives like the UBR strive to enhance transparency in Kenya's business and financial sector, implementation challenges and limited awareness among stakeholders impede their efficacy.

Moreover, the digital financial spaces introduce potential avenues for ML, with anonymous virtual transactions, crypto-currencies, and the CBDC posing significant risks. These advancements could empower criminals to blur their transaction trails and mask the origin of illicit funds, further complicating efforts by regulators and law enforcement agencies. Addressing these challenges necessitates a multifaceted approach involving robust regulatory frameworks, enhanced collaboration among stakeholders, and comprehensive awareness campaigns. Strengthening AML measures, improving regulatory oversights and capabilities, and fostering greater transparency in financial transactions are imperative to mitigate the risks posed by evolving patterns of illicit financial flows in Kenya. By addressing these issues proactively, Kenya can bolster her financial integrity and safeguard against the detrimental impacts of ML.

Recommendations

On TBML and FBML

1. The Office of Prime Cabinet Secretary:
   i) Enhance collaboration and cooperation among relevant stakeholders, including religious entities, government agencies, regulatory bodies, financial institutions, and law enforcement agencies on combating TBML and FBML
   ii) Work closely with other countries and international organizations to share best practices and intelligence, and enhance international cooperation in combating TBML and FBML.
   iii) Invest in capacity building and training programs for relevant stakeholders, to enhance their understanding of TBML and FBML techniques, develop effective investigation skills, and keep up with evolving trends.
   iv) Coordinate investments in advanced technological solutions that can help identify suspicious trade patterns, flag potential TBML and FBML cases, and improve the efficiency of investigations.

2. The Financial Reporting Centre should raise public awareness about the risks of TBML and FBML and promote a culture of compliance and transparency within the business community.

On UBR

1. The Office of the Prime Cabinet Secretary should foster partnerships between relevant government agencies, regulatory bodies, and financial institutions to share information and ensure a consistent and accurate flow of UBO data.

2. The Financial Reporting Centre should raise public awareness about the risks of TBML and FBML and promote a culture of compliance and transparency within the business community.
   i) Conduct extensive awareness campaigns and guide companies and individuals on their obligations regarding UBO reporting and the importance of maintaining accurate and up-to-date UBO information.
   ii) Ensure the fortification of cyber-security measures to ensure the UBR's software and systems remain secure against known and emerging vulnerabilities.

Recommendations

In the digital space

1. The CBK should establish and roll out a comprehensive regulatory framework specifically tailored to the digital payment industry.

2. The Capital Markets Authority (CMA) should lobby the National Parliament and the Senate to debate and pass the Capital Market Authority Amendment Bill (2023) that will mainstream the regulation of the cryptocurrency market in Kenya.

3. The Ministry of Information, Communications, and the Digital Economy and the CMA should spearhead public awareness campaigns and educational programs to educate citizens and business entities on the risks of ML associated with the online space.

THE GLOBAL CENTRE FOR POLICY AND STRATEGY
(GLOCEPS)
Research | Knowledge | Influence

Off Kiambu Road, Nairobi Kenya
P.O. Box 27023-00100,Nairobi.
Telephone: 0112401331
Email: info@gloceps.org
Web: www.gloceps.org